Strategy Research Project

Department of Defense Synchronization and Coordination via Joint Information Environment

by

Colonel Ivan Montanez
United States Army

United States Army War College
Class of 2013

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
xx-03-2013

2. REPORT TYPE
STRATEGY RESEARCH PROJECT

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Department of Defense Synchronization and Coordination via Joint Information Environment

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Ivan Montanez
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor Brian Gouker
Department of Military Strategy, Planning, & Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5,468

14. ABSTRACT

The United States has endured a turbulent period, one dominated by the 9/11 attacks. America must continue to prepare for these malicious attempts as these actors attempt to disrupt, destroy, and attack the networks and communication systems that enable the DoD to control systems. The very technologies that empower us also empower our adversaries and diminish our ability to respond to natural disaster and military contingencies. The U.S. needs for networks that are secure, trustworthy, and resilient that enables an information sharing environment. To mitigate the lack of an information sharing environment, it is essential that the Department of Defense (DoD) develop dependable, trustworthy and resilient networks, while improving response to cyber incidents, and enhancing operability, interoperability and synergy across all domains. The DoD has realized that the application of technology will enable all stakeholders the ability to share, synchronize, and collaborate information while enhancing mission performance and execution. Hence, the need for a Joint Information Environment (JIE) that will leverage the use of new technologies, to improve operational effectiveness, cost-efficiency, and security.

15. SUBJECT TERMS
Information Sharing, Effective, Efficient, Secure Networks

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU	30	**19b. TELEPHONE NUMBER** *(Include area code)*

USAWC STRATEGY RESEARCH PROJECT

Department of Defense Synchronization and Coordination via Joint Information Environment

by

Colonel Ivan Montanez
United States Army

Professor Brian Gouker
Department of Military Strategy, Planning, & Operations
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Department of Defense Synchronization and Coordination via Joint Information Environment
Report Date:	March 2013
Page Count:	30
Word Count:	5,468
Key Terms:	Information Sharing, Effective, Efficient, Secure Networks
Classification:	Unclassified

The United States has endured a turbulent period, one dominated by the 9/11 attacks. America must continue to prepare for these malicious attempts as these actors attempt to disrupt, destroy, and attack the networks and communication systems that enable the DoD to control systems. The very technologies that empower us also empower our adversaries and diminish our ability to respond to natural disaster and military contingencies. The U.S. needs for networks that are secure, trustworthy, and resilient that enables an information sharing environment. To mitigate the lack of an information sharing environment, it is essential that the Department of Defense (DoD) develop dependable, trustworthy and resilient networks, while improving response to cyber incidents, and enhancing operability, interoperability and synergy across all domains. The DoD has realized that the application of technology will enable all stakeholders the ability to share, synchronize, and collaborate information while enhancing mission performance and execution. Hence, the need for a Joint Information Environment (JIE) that will leverage the use of new technologies, to improve operational effectiveness, cost-efficiency, and security.

Department of Defense Synchronization and Coordination via Joint Information Environment

> Future Joint Forces will face an increasingly complex, uncertain, competitive, rapidly changing, and transparent operating environment characterized by security challenges that cross borders. Joint force elements postured around the globe can combine quickly with each other and mission partners to harmonize capabilities fluidly across domains, echelons, geographic boundaries, and organizational affiliations. The assertion is that through globally integrated operations, Joint Forces will remain able to protect U.S. national interests despite constrained resources.
>
> —GEN Martin E. Dempsey
> Chairman of the Joint Chiefs of Staff

The United States has endured and continues to work through a turbulent period, one dominated by the 9/11 attacks, the war on terrorism, the wars in Iraq and Afghanistan and natural disaster events. These events at home and abroad have characterized the strategic environment as one that is volatile, uncertain, complex, and ambiguous (VUCA). The events also present broad National Security challenges that test America's stability, resiliency and ability to respond promptly to events. Globalization, "the process of interaction and integration among the people, companies, and governments of different nations, a process driven by international trade and investment and aided by information technology,"[1] has facilitated free nations, open markets, and social growth throughout the world. It has also enabled nations, non-state actors and failed states to compete and determine their own destiny. As Thomas Friedman stated it, "Suddenly more people from more different places could collaborate with more other people on more different kinds of work and share more different kinds of knowledge than ever before."[2] The power of technology to connect, compete, collaborate, and unfortunately destroy[3] has accelerated globalization at an extraordinary rate, empowering individuals for good and bad.

America must be prepared for malicious actors who attempt to disrupt, destroy, and attack the networks and communication systems that enable us to control systems at home and abroad. The very technologies that empower us to lead also empower America's adversaries and diminish our ability to respond to natural disaster, military contingencies and emergencies quickly. In this environment U.S. needs for networks that are secure, trustworthy and resilient.

To mitigate the lack of a dependable communications infrastructure that allows for information sharing, it is essential that the Department of Defense (DoD) develop dependable, trustworthy and resilient networks, while improving response to cyber incidents, reducing threats and vulnerabilities, and enhancing operability, interoperability and synergy across all domains (air, sea, land, space, cyber). Unfortunately, the way the DoD networks are developed, funded, and implemented fosters unnecessary complexity and redundancy. As a result of this decentralized approach and lack of governance and oversight, the DoD's Information Technology (IT) infrastructure delivers a patchwork of capabilities that create cyber vulnerabilities, impedes joint operations, results in large cumulative costs, and limits the ability to capitalize on the "promise of IT".[4] The current DoD IT environment is dominated by independently stovepiped, developed, acquired and managed component and installation specific capabilities. The DoD will need to ensure that its limited resources are aligned to the requirements in support of a globally networked infrastructure in which the DoD, service components and agencies can interoperate, collaborate, share secure information and are synchronized with all instruments of U.S. national power. The DoD must change its core processes to address these systemic conditions to achieve a secure Joint Information Environment (JIE).

The "JIE is comprised of shared information technology (IT) infrastructure, enterprise services, and single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security and realize efficiencies."[5] Department of Defense (DoD) Chief Information Officer's (CIO) vision is for a more effective, efficient and secure Information Enterprise. This environment will give decision makers access to persistent, continuously available, collaborative and knowledge management capabilities, access they need to exercise authority and direct mission execution.

In an effective JIE, all efforts would be integrated, coordinated and synchronized throughout all levels of the DoD. To achieve this, the DoD is investing and improving the reliability, security, and interoperability of communication systems across the DoD, Military Services and Geographical Combatant Commands (GCC). This will facilitate the synchronization and collaboration, which is required to operate in a contested environment.

In an uncertain strategic environment, the DoD has recognized the need to be more agile. In a JIE, the DoD seeks to create a collaborative environment that encourages better sharing of information across all domains.[6] One step towards better sharing of information is combining service capabilities across domains, which will enable collaboration and sharing of information across the DoD, allowing our allies and partners to work independently but in consonance with national authorities, under their guidance and intent. This is called cross-domain synergy, "the complementary of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of others."[7] America's leadership seeks to protect freedom of access throughout the domains by maintaining relevant and interoperable military capabilities that will enable the DoD to coordinate, synchronize, collaborate and share secure information. Cross domain synergy also facilitates the employment of information operations (IO), which supports full spectrum dominance by taking advantage of information technology, maintaining U.S. strategic dominance in network technologies, and capitalizing upon near real-time global dissemination of information. The goal of cross-domain synergy is to affect adversary decision cycles, thus achieving information superiority for the United States.[8]

In order to gain a clear understanding and appreciation of the concerted efforts of all instruments of national power required to meet challenges of current and future operations, the DoD needs to evolve to meet the challenges within the information environment. This environment includes the Armed Forces of the United States, United States Government (USG) departments and agencies, state, territorial, local, and tribal government agencies, foreign military forces and government agencies, intergovernmental organizations (IGOs), nongovernmental organizations (NGOs), and entities of the private sector. This environment will improve unity of effort, a reduction in decision time, increased adaptability of forces, improved situational awareness, and greater precision in mission planning and execution.[9] To attain a common virtual space in which all communities of interest (COI) can collaborate and share information across-domains will require the stand up of communities of interest (COI) to recognize and treat information as a strategic asset.

Culture of Information in Joint Information Environment (JIE)

For the JIE to have its intended effect, the culture will have to shift from owning to sharing information throughout the DoD. There is an established mindset of information “ownership” when the new mindset must be one of information “stewardship”. The best technology, processes, and policies will not make this successful if the people do not embrace the new cultural norms. To facilitate this shift, organizational leaders must support this cultural change, set the example, educate their people, and offer incentives for, and enforcement of information sharing and stewardship. The organizational approach and philosophy to adopt a sharing posture must be driven through shared missions and the ability and flexibility to “realign” and adapt to changing circumstances.[10]

An example of government agencies that embraced the JIE like sharing concept occurred when The Department of Defense (DoD), Department of Homeland Security (DHS), and Department of Transportation (DOT) developed a partnership to manage the visibility and access to information related to the global maritime domain. All three departments acknowledged that it was not practical for each of them to solve these problems independently, so they developed a community of interest (COI) to address the challenges. The COI agreed and demonstrated four principals that underscore the power of information sharing. Leaders in the DoD, DHS and DOT recognized and treated information as a strategic asset. They recognized that establishing a shared network infrastructure would involve a difficult culture shift for senior managers and workers, from one of owning information to one of sharing information. The DoD, DHS and DOT were willing to change their current applications, services and databases to shift from stovepipe, highly tailored, and individually engineered systems to an architecture that allows data and services to be accessed through a common shared virtual space by authenticated users. Finally, they identified those willing individuals within their agencies who wanted to establish common information parameters, which established a common process and determined the technology they would use.[11]

As a result of this common process, the COI was able to use the national maritime common operational picture (COP). The COP is a near-time, dynamically tailorable, network-centric virtual information grid shared by the agencies that have maritime interests and responsibilities. COP data is accessible to all users and currently contains some decision-maker toolsets. Additional toolsets and enablers will enhance this capability and will eventually be synchronized with the other domains. This is the first step in support of the national plan to achieve Maritime Domain Awareness (MDA) by the DoD, DHS and DOT. The MDA COI is creating an environment that is conducive towards an effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, and environment of the United States. It is an essential component of an active, layered maritime defense in depth, that will improve the ability to collect, fuse, analyze, display, and disseminate actionable information and intelligence to operational commanders.[12]

The JIE concept is a very complicated undertaking, but the DoD is using another system that has laid the foundation for an integrated networking environment – the enterprise email system led by the Army and the Defense Information Systems Agency (DISA). The entire Joint Staff uses enterprise email, and the Army has migrated most of the U.S. Army personnel. The Army has been moving geographically - dispersed email systems run by individual commands and military bases into a new system in the cloud operated by the DISA. One other enterprise system to follow the enterprise email is a portal service based on Microsoft SharePoint platform. The service allows users to collaborate, and share information in a secure environment.

These success stories are just the beginning of a complicated but rewarding effort. Integrating the JIE concept across all domains emphasizes the cross-domain synergy, which implies a degree of joint interdependence at relatively all levels and will demand a robust command and control (C2) system and a major investment in frequent and realistic training. In an era of constrained defense budgets, the JIE concept will require an initial significant resource investment due to its resource-intensive requirements. The initial investment will deliver a desired capability that will facilitate command and control through mission command (MC). "Mission Command is the exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the commander's intent to empower agile and adaptive leaders in the conduct of unified land operations."[13] The robust infrastructure JIE is being designed to deliver will support the mission command philosophy by providing a collaborative, synchronized, information-sharing environment that will provide for timely, relevant, secure information, and situational awareness to the component commander's. The risk with the initial investment is worth taking with the understanding that it will increase operational effectiveness and cost efficiencies.

All the DoD organizations and government agencies face increasingly complex requirements concerning the management and sharing of information. Throughout time, all systems have been engineered for particular functions within an organization, which in most cases limited the ability for information sharing and collaboration. These challenges have been recognized by each particular organization to include the critical concern of security for these systems. In a pertinent example during Hurricane Katrina, problems with communications operability and interoperability constituted one of the main reasons for government's failures in response. Operability refers to the basic functionality of any device while interoperability refers to the device's ability to connect with other devices and share voice or data communications. Mississippi Governor Haley Barber summed up the lack of information sharing and communications: "My head of the National Guard might as well have been a Civil War General for the first two or three days because he could only find out what was going on by sending somebody. He did have helicopters instead of horses, so it was a little faster but the same sort of thing."[14] To attain secure cross-domain synergy that overcomes these risks will require a greater degree of integration than ever before with the DoD, interagency and foreign partners and a change of attitude towards change itself.

The growth of disparate networks within the DoD and agencies increase the system vulnerabilities while increasing risks throughout the domains. Technology's rapid advances make the elimination of all vulnerabilities impossible. However, to address the evolving threats and increased risks, the DoD governmental agencies need to work together to enhance their cybersecurity postures. Cyberspace touches nearly every part of our daily lives. It is the broadband network beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation; the classified military and intelligence networks that keep us safe and the World Wide Web (www) that has made us more interconnected than at any time in human history. We must secure cyberspace to ensure that we can continue to grow the nation's economy, protect the American's national interest and her way of life. "Extending the principles of peace and security to cyberspace will require strengthened partnership and expanded initiatives."[15]

Threats to Information in the JIE

Unfortunately, an integrated JIE will experience risks of disruption and attack by both state and non-state actors who possess the capability and intent to conduct cyber espionage and, potentially, cyber attacks on the United States, with possible severe effects on both military operations and our homeland.[16] Some of these threats can cause total system failure, therefore, detecting, deterring and defending against cyber attacks is essential to protecting the DoD's communication infrastructure and information. We rely on an array of networks, yet theft of intellectual property, cyber intrusions and attacks have increased dramatically, exposing the DoD's and agencies' sensitive infrastructure and information. President Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity."[17] A Cyber attack is a critical concern for all senior leaders. Attacks are on the rise and can cause significant setbacks and critical information losses. Different actors who are motivated by different interests conduct cyber attacks, and the attacks increase by the day.

A Government Accounting Office (GAO) report states that the number of incidents reported by federal agencies to the federal information security incident center has increased by nearly 680%, over the past six years. In numerical terms, some 42,887 incidents were recorded in 2011, up from just 5,503 in 2006.[18] In September 20, 2012 an article was published detailing some of the events occurring in the last three years. The report, which was released by private security firm Rapid 7 and based on data collected by the Privacy Rights Clearinghouse, focused on the period of January 1, 2009 through May 31, 2012. During that time, there were 268 reported breach incidents in government agencies. The federal government has reported unintentionally exposing more than 94 million records containing personally identifiable information. In the first half of 2012, government data breaches represented 14 percent of all incidents, with private enterprise claiming 64 percent of the reported incidents, according to The Open Security Foundation's DataLossDB. The Rapid7 report characterized government security controls and best practices as “weak”, and security costs as growing.[19]

Malicious actors target government agencies and networks to obtain information that can compromise the security of the Armed Forces in general or a particular mission, or to gain intellectual insights to US programs. Frequently hit targets include the US Department of Defense, the Pentagon, NASA, Los Alamos Laboratories, Boeing, Lockheed Martin, Northrop Grumman, Raytheon, Harvard University, California Institute of Technology, and a wide range of think tanks, defense contractors, military installations, and high profile commercial corporations. These malicious actors have often been able to steal classified data, such as naval codes, information on missile guidance systems, personnel performance reports, weapons development, and descriptions of the movement of equipment and personnel. The United States of America’s paramount position and its heavy reliance on computers have made it a prime target. For this reason, it has been the target of some of the most extensive cyber attacks. “The United States has had millions of computers infected at a cost in the billions of dollars.”[20]

Many of these attacks are aimed at the DoD infrastructure and its agencies to probe the resiliency of the network infrastructure and security of its information. A recent article in the New York Times describes the persistent attacks the nation, state and commercial infrastructures are exposed to every day. Specifically a significant number of government agencies and commercial websites from the United States and South Korea were recently jammed. The attacks were identified as unsophisticated and their origin could not be identified but still affected 50 to 60 thousand computers, which caused them to slow down or stall.

> The Web sites of the Treasury Department, Secret Service, Federal Trade Commission and Transportation Department were all affected. The Web sites of the Treasury Department, Secret Service, Federal Trade Commission and Transportation Department were all affected. The attacks focused on the small group of United States government Web sites, but the list later expanded to include commercial sites in the United States and then commercial and government sites in South Korea.[21]

Should a more sophisticated attack take place in the United States, a significant portion of the attacks could be directed at the DoD, military forces, and/or agency’s networks.

If a cyber attack disabled systems within the DoD or military departments, it could be devastating and would result in a major delay in notification, response, and dispatch of proper authorities to a given event, which could cause unnecessary loss of life and property. It is not surprising that the DoD’s networks have become targets. Through time, the attacks can be expected to increase in an attempt to test the level of security and protection of the DoD’s communication infrastructure. Therefore, the DoD must continue to be vigilant and prepared to react nearly instantaneously to effectively limit the damage that the most sophisticated types of attacks can inflict. Hence, the need for the DoD, partners and allies to commit the necessary resources to build cybersecurity capacity across the range of networks, communication infrastructures and collaborative environments.[22]

As the DoD becomes more dependent on information sharing capabilities in a JIE, our adversaries are motivated to exploit and disrupt information sharing, threaten the command and control channels, and deny the use of information and communications infrastructure. The enemy is ready to react whenever the Department deploys new defensive postures, hence the reason to enhance the cybersecurity posture at home and abroad. "There will never be a time that we assume a 'comfort' zone."[23] Therefore, the implementation of the protection warfighting function is required to preserve the force and physical assets of the United States, host-nation, and multinational military and civilian partners.[24]

In this environment, the DoD needs to develop strategies, policies, authorities, capacity and capabilities to manage and defend its information networks.[25] While Chief Information Officers (CIOs) want to ensure that information is visible, accessible, and understandable to all authorized users, government organizations need to ensure that the information is shared in a trusted environment. Lack of security can interfere with vital information sharing within the DoD. As a result, the government has the responsibility to address the strategic vulnerabilities to ensure that the DoD realizes the full potential of information technology. How the government looks at the security of the systems is critical before, during and after the engineering and operation of future networks. As important as it is for the information technology workforce to understand cybersecurity, it is as important that leaders at all levels of government understand the risks and potential impacts that lack of cybersecurity can cause and the importance of building and operating networks that can identify and respond to cyber degradation and/or attack.

Meeting Cybersecurity Challenge to the JIE

To meet these challenges, military and the DoD senior leaders must think and act as a single enterprise, rather than a set of discrete organizations. To achieve this enterprise mindset, the DoD must work collaboratively with key leaders and stakeholders to develop government wide strategies to achieve unity of purpose. They must champion enterprise capabilities where appropriate and establish strong but lean governance to ensure that our information capabilities are interoperable across the DoD and with our mission partners.

> The National Strategy to secure Cyberspace articulates five national priorities. "The first priority focuses on improving our ability to respond to cyber incidents and reduce the potential damage from such events. The second, third, and fourth priorities aim to reduce the numbers of cyber threats and our overall vulnerability to cyber attacks. The fifth priority focuses on preventing cyber attacks with the potential to impact national security assets and improving international management of and response to such attacks."[26]

As a result, awareness through education and continuous cyber security improvement will incrementally reduce threats and vulnerabilities throughout the DoD systems and networks, which will result in protection of the information being shared outside and inside of the department.

The warfighter expects and deserves access to information from any device, anywhere, anytime. Consequently, it is critical to move to a Joint Information Environment (JIE) that will "enable the DoD, agencies, service components, component commander's and civilian leaders to act quickly and effectively, in concert with multiple mission partners, based on the best, most accurate, and timely information available."[27] We must enable them with powerful capabilities that allow for collaboration and synchronization across the Joint, Interagency, Intergovernmental, and Multinational (JIIM) environment as rapidly as possible, without compromising safety and security.[28] Information must be treated as a strategic asset to ensure information capabilities are available throughout and in support of the DoD, agencies, service components, allies and partners.

GEN Dempsey, Chairman of the Joint Chief of Staff (CJCS), speaks to the importance of developing and investing in a globally integrated operations concept.[29] He recognizes that all elements of national power have to be integrated in order to have any operational success at home or abroad. GEN Dempsey affirms that, "in many cases strategic success will turn on our ability to operate in concert with the rest of the U.S. government, allied governments and their armed forces and nongovernmental partners."[30] To achieve this concerted operation, aggressively transition from a single strand mission support capabilities managed by different organizations spread to an effective, efficient and secure environment, one that will synchronize capabilities across domains, echelons, geographic boundaries, and organizational affiliations. "The Department must transform information technology (IT) solutions, deployments, and operations to enterprise IT services, and establish them as on-demand services that are scalable, diverse, and offered as a managed package to support every need within the DoD."[31] It must streamline the process by which information capabilities are developed, acquired, secured, and fielded. In the face of a declining budget, the department must make hard decisions about which initial investments to fund that will improve effectiveness and gain efficiencies throughout all entities.

The DoD and the combatant commander demand timely access and collaboration of information, which synchronizes all efforts to improve mission performance and effectiveness. The benefits of the JIE are aimed at achieving improved mission effectiveness and cybersecurity. "The Joint Information Environment is a robust and resilient enterprise that delivers faster, better-informed collaboration and decisions enabled by secure, seamless access to information regardless of computing device or location."[32] These benefits will facilitate agile, rapid delivery of effective, secure information capabilities across all missions and warfighting functions. These capabilities will leverage the best IT available to support the increased, ever-evolving information demands of the users. The JIE concept will establish proactive measures that remove barriers to network access and information sharing between all beneficiaries, reducing the existing network obstacles that impede our ability to effectively, securely share information, and have mission success.

Given the complexity of this environment and the different organizations involved with the JIE concept, it is imperative that stakeholders or communities of interests (COI) work together. Building the necessary relationships will allow for shared approaches to implementing, maintaining, sharing and securing the capabilities, services, and products that support the range of military and domestic operations. Together, the DoD components must have one vision supported by policy, standards and engineering in the form of unified guidance. Teri M. Takai, Department of Defense (DoD) Chief Information Officer (CIO) mentions that "The next tier of this relationship is the network and services management partnership forged between the Department of Defense Chief of Information Officer (DoD CIO), the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)), and the DoD Components"[33] This strong, collaborative affiliation capitalizes on the strength of each other to figure out what best works for all.

The DoD CIO provides information resources policy, while the USD (AT&L) provides acquisition policy and program oversight functions. DISA and other the DoD Components focus on acquiring, building, and securing our networks and services. In the operational side of this partnership, the DoD CIO works with United States Cyber Command (USCYBERCOM) to provide oversight functions to all the DoD organizations that operate and defend the DoD networks. These organizations work together to leverage the three major decision processes: requirements, budget, and acquisition processes. Finally, there is the secure information sharing responsibility with the DoD Components, joint, interagency, intergovernmental, and multinational. The collaboration and synchronization of these groups will achieve cross-organizational information sharing, while securing sensitive information and addressing threats and vulnerabilities to global infrastructure.[34] It will also enable all stakeholders to do more with less as they invest in promising programs that will deliver capability quickly to the warfighter.

The DoD components have realized the importance of working as a team to develop an information environment that supports leaders at home and abroad during peacekeeping operations, domestic disasters, or contingency operations. They have come to the realization that the application of technology will enable all stakeholders to share, synchronize, and collaborate information enhancing mission performance and execution. GEN Dempsey says, that “New technologies, appropriately applied, can improve operational effectiveness, efficiency, and security.”[35] Finally, even as decision makers and leaders across the DoD must work together towards delivering capability, they must rapidly and boldly terminate programs with outdated technology that refuse to field the latest technology quickly, or those that do not comply with the DoD’s technical standard.

Conclusion and Recommendation

It is clear that to operate in a complex environment the DoD, agencies, service components, component commander’s and civilian leaders will benefit by sharing a common secure information environment. This cooperation will facilitate agile, rapid delivery of effective, secure information capabilities across all missions and functions. The ability to collaborate and synchronize across all entities will allow for combining unique Service capabilities into a coherent operational whole.[36] The Joint Information Environment will provide an environment that will add an advantage across multiple functional areas through the integration, innovation, and consolidations of IT systems while at the same time improve the overall DoD security posture. The DoD has the responsibility to ensure that all stakeholders within the DoD, component commander’s, services, allies and partners share common IT services and that the enterprise services are provided in the most cost-efficient manner possible. The DoD organizations, as mentioned earlier in the paper, have demonstrated “that leveraging shared services and consolidating IT and telecommunications equipment, resources, and investments can improve efficiency, cost-effectiveness, and environmental sustainability in IT and telecommunications operations.”[37] More integrated systems and networks will reduce the lack of information sharing and improved interoperability, security, and overall operational effectiveness and efficiency.

The recommendation is simple. In order to achieve the JIE concept the Department of Defense (DoD) should review all areas of the budget for potential savings. It is highly encouraged that the DoD divest in all areas of the network and communication enablers that are duplicative in nature. Develop a strategy that will conform to the future force structure and in support of the network/communications, and information sharing modernization efforts. The strategy will also realize efficiencies across the department, enhance contract competition and will force all services to reevaluate their modernization programs. Through the information technology (IT) procurement and review and approval process, the DoD needs to monitor every dollar planned for IT and ensure that it is properly invested in support of the JIE concept. This will assist the department to identify redundant missions and programs and force them to set priorities and make hard choices. It will require our senior leaders to direct the termination of certain programs that have incurred a high cost through time and are duplicative throughout the services and that have not delivered the promised capability. These actions need to occur so that there can be an initial investment that delivers enterprise services, creates credibility throughout the department, while delivering effective services to the DoD and the services. Additionally, senior leaders will need to assess and accept some risk to allow for an effective, efficient while secure Joint Information Environment (JIE). One that will provide the environment necessary that will empower our leaders to have access and share the required information to make timely decisions.

Endnotes

[1] Globalization 101, What is globalization, http://www.globalization101.org/what-is-globalization (accessed January 26, 2013)

[2] How globalization is changing the world, http://www.centerforpubliceducation.org/Learn-About/21st-Century/How-globalization-is-changing-the-world.html (accessed January 6, 2013).

[3] Thomas L. Friedman, *The World is Flat, A Brief History of the Twenty-first Century* (New York, NY: Picador / Farrar, Straus and Giroux), 665.

[4] Teri M. Takai, *Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap* (Washington DC: U.S. Department of Defense, September 2011), 2.

[5] Joint Information Environment Sponsor Group, *Joint Information Environment Concept of Operations* (Washington DC: Joint Operations Sponsor Group, October 2012), 6.

[6] U.S. Department of Defense Chief of Information Officer, "*Information Sharing Successes*," video file. http://dodcio.defense.gov/Portals/0/videos/CIO3.mpeg (accessed January 12, 2013)

[7] U.S. Joint Chief of Staff, *Joint Operational Access Concept* (Washington DC: Joint Chief of Staff, January 12, 2012), ii.

[8] William J. Lynn III, *Department of Defense Directive DoDD 3600.1, Subject: Information Operations* (Washington DC: Department of Defense, August 2006), 2.

[9] John G. Grimes, *Department of Defense Information Sharing Strategy* (Washington, D.C: Office of the Chief Information Officer, October 2007), ii.

[10] Ibid., 10.

[11] U.S. Department of Defense Chief of Information Officer, "*Information Sharing Successes*," video file. http://dodcio.defense.gov/Portals/0/videos/CIO3.mpeg (accessed January 12, 2013)

[12] U.S. Department of Defense, *National Plan to Achieve Maritime Domain Awareness,* (Washington, DC: U.S. Department of the Army, October 2005), ii.

[13] U.S. Department of the Army, *Mission Command*, Army Doctrine Publications 6-0 (Washington, DC: U.S. Department of the Army, May 17, 2012), 1.

[14] Special Report of the Committee on Homeland Security and Governmental Affairs, S. Rept. 109-322 "Hurricane Katrina: A Nation still Unprepared", 109th Congress, 2nd Session. Available at http://www.gpo.gov/fdsys/pkg/CRPT-109srpt322/pdf/CRPT-109srpt322.pdf (Accessed January 26, 2013)

[15] President Barack Obama*, International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World*, (Washington, DC: The White House, May 2011), 11.

[16] Leon E. Panetta, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: The White House, January 2012), 3.

[17] National Security Council, “Cybersecurity,” March 9, 2009. http://www.whitehouse.gov/administration/eop/nsc/cybersecurity (accessed January 19, 2013).

[18] Alex Wilhelm, “Cyber attacks on the federal government up 680% in the last 6 years,” April 25, 2012, http://thenextweb.com/us/2012/04/25/cyber-attacks-on-the-federal-government-up-680-in-the-last-6-years/ (accessed January 19, 2013).

[19] News Staff, “Report: Feds Exposed 94 Million Records in 3 Years,” September 20, 2012, http://www.govtech.com/security/Report-Feds-Exposed-94-Million-Records-in-3-Years.html (accessed January 19, 2013).

[20] Jason Fritz, “How China will use Cyber Warfare to Leapfrog in Military Competitiveness”, October 2008, http://www.international-relations.com/CM8-1/Cyberwar.pdf (accessed January 19, 2013), 54.

[21] Choe Sang-Hun and John Markoff, ” Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea,” July 8, 2009, http://www.nytimes.com/2009/07/09/technology/09cyber.html?_r=0 (accessed January 19, 2013).

[22] President Barack Obama*, International Strategy for Cyberspace, Property, Security, and Openness in a Networked World*, (Washington, DC: The White House, May 2011), 15.

[23] Teri M. Takai, *Department of Defense (DoD) Chief Information Officer (CIO) Campaign Plan Summary* (Washington DC: U.S. Department of Defense, Fiscal Year (FY) 2013), 4.

[24] U.S. Department of the Army, *Unified Land Operations*, Army Doctrine Publication 3-0 (Washington, DC: U.S. Department of the Army, October 2011), 14.

[25] Robert M. Gates, Quadrennial Defense Review (Washington, DC: U.S. Department of Defense, February 2010), 37.

[26] George W. Bush, *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, February 2003), 3.

[27] Takai, *Department of Defense (DoD)*, 1.

[28] Takai, “Department of Defense (DoD)”, 1.

[29] GEN Martin E. Dempsey, *Capstone Concept for Joint Operations: Joint Force 2020* (Washington, DC: U.S. Department of Defense, 10 September 2012), 4.

[30] Ibid., 1.

[31] Takai, “Department of Defense (DOD),” 4.

[32] Teri M. Takai, *Cloud Computing Strategy* (Washington DC: U.S. Department of Defense, July 2013), E-1.

[33] Takai, “Department of Defense (DOD),” 6.

[34] GEN Dempsey, “Capstone Concept for Joint Operations,” 6.

[35] Ibid., 7.

[36] GEN Dempsey, “Capstone Concept for Joint Operations,” 16.

[37] Takai, “Department of Defense (DoD) Information Technology (IT),” 9.